

United States District Court

NORTHERN DISTRICT OF TEXAS

JAN 22 2016

CLERK, U.S. DISTRICT COURT
APPLICATION AND AFFIDAVIT
FOR SEARCH WARRANT

In the Matter of the Search of

Information associated with the account @JusticeSeeker01, with URL <https://twitter.com/justiceseeker01>, which is stored at premises controlled by Twitter, Inc., at 1355 Market Street, Suite 900, San Francisco, California

CASE NUMBER:

0:16-mj-46-BF

I, Federal Bureau of Investigation Special Agent Sheraun P. Howard being duly sworn depose and say:

I am a Federal Bureau of Investigation Special Agent and have reason to believe that on the property or premises described as follows:

Information associated with the account @JusticeSeeker01, with URL <https://twitter.com/justiceseeker01>, which is stored at premises controlled by Twitter, Inc., at 1355 Market Street, Suite 900, San Francisco, California, further described in Attachment A.

in the Northern District of California there is now concealed a certain property, namely those more specifically described in the attached Attachment B which are the evidence, fruits, and instrumentalities of crimes concerning violations of 18 U.S.C. §§ 1030(a)(5)(A) and 1030(b).

The facts to support a finding of Probable Cause are as follows:

SEE ATTACHED AFFIDAVIT.

Signature of Affiant

SHERAUN P. HOWARD

Special Agent, Federal Bureau of Investigation

Sworn to before me, and subscribed in my presence

January 22, 2016

Date and Time Issued

at Dallas, Texas

City and State

PAUL D. STICKNEY, U.S. Magistrate Judge

Name and Title of Judicial Officer

Signature of Judicial Officer

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, Sheraun P. Howard, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for warrants to search the information associated with the Twitter account **@JusticeSeeker01**, **<https://twitter.com/justiceseeker01>** (Twitter Account). The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Twitter Inc., to disclose to the government copies of the information (including the content of communications) further described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

2. I am a Special Agent with the Federal Bureau of Investigation (FBI), duly appointed and acting according to law. I have been employed as a Special Agent of the FBI since November 2008. Prior to becoming a Special Agent, I was employed by the FBI as an Intelligence Analyst. Since May 2009, I have been assigned to investigate violations of federal law including violations involving computer/high technology crime including malicious computer activity, computer intrusions, and internet related fraud schemes. During my employment as a Special Agent and Intelligence Analyst, I have received hands on training in investigating computer

crime for the FBI. As a federal agent, I am authorized to investigate violations of United States laws and to execute warrants issued under the authority of the United States. I am currently assigned to the Dallas Division of the FBI, where I have been tasked to investigate computer crimes, including computer intrusions.

3. The facts in this affidavit come from my personal observations, my training and experience. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

4. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that evidence, fruits, and instrumentalities of violations of 18 U.S.C. §§ 1030(a)(5)(A), are presently stored at premises owned, maintained, controlled, or operated by Twitter, Inc., headquartered at 1355 Market Street, Suite 900, San Francisco, CA 94103. There is also probable cause to search the information described in Attachment A for evidence of these crimes further described in Attachment B.

JURISDICTION

5. This Court has jurisdiction to issue the requested warrant because it is a “court of competent jurisdiction” as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A) & (c)(1)(A). Specifically, the Court is a district court of the United States . . . that – has jurisdiction over the offense being investigated.” 18 U.S.C. § 2711(3)(A)(i).

6. There is probable cause to believe that violations of 18 U.S.C. §§ 1030(a)(5)(A) have occurred.

a. 18 U.S.C. § 1030(a)(5)(A) provides the following:

Whoever—knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization to a protected computer... [shall be punished in accordance with law].

A “**protected computer**” is defined at 18 U.S.C. § 1030(e)(2)(B) in pertinent part as “a computer used in or affecting interstate or foreign commerce or communication

The term “**damage**” is defined at 18 U.S.C. § 1030(e)(8) as “any impairment to the integrity or availability of data, a program, a system, or information.”

GLOSSARY OF TERMS

7. I use the following terms related to computer/communication networks in this affidavit:

- a. **Tweet:** (Digital Technology) A very short message posted on the Twitter website: the message may include text, keywords, mentions of specific users, links to websites, and links to images or videos on a website.
- b. **Hashtag:** (On social-networking websites) A word or phrase preceded by a hash mark (#), used within a message to identify a keyword or topic of interest and facilitate a search for it. (On the Twitter website) A word or phrase preceded by a hash mark, used to denote the topic of a post.
- c. **Domain Name:** (Computers) A name owned by a person or organization consisting of an alphanumeric sequence followed by a suffix indicating the top level domain: used an Internet address to identify the location of particular Web pages.

- d. **Denial of Service (DoS):** Pertaining to or being an incident in which a computer or computer network is disabled, disrupting access or service.
- e. **Distributed Denial of Service (DDoS):** A type of DoS attack where multiple compromised systems (computers, etc.) are used to target a single system causing a DoS attack
- f. **Standard Query Language (SQL):** A special-purpose programming language designed for managing data held in a relational database management system.
- g. **SQL Injection:** A code injection technique, used to attack data-driven applications, in which malicious SQL statements are inserted into an entry field for execution (e.g. to dump the database contents to the attacker).
- h. **Remote Desktop Protocol (RDP):** A proprietary protocol developed by Microsoft, which provides a user with a graphical interface to connect to another computer over a network connection. The user employs RDP client software for this purpose, while the other computer must run RDP server software.
- i. **Secure Shell (SSH):** An encrypted network protocol to allow remote login and other network services to operate securely over an unsecured network.

PROBABLE CAUSE

1. On January 25, 2015, Longview, Texas Police Department (LPD) notified the FBI of attacks to their computer network. LPD stated they believed the attacks were in retaliation for the recent LPD fatal shooting of a 17 year old female, Kristiana Coignard, in the lobby of the LPD station January 22, 2015, after Coignard brandished a knife in aggravation against the officers. On January 24, 2015, LPD received a comment on their official Facebook account from another Facebook user

stating that they were a member of the hacking collective Anonymous, and inferred that they would retaliate for the fatal shooting of Kristiana Coignard.

2. At approximately 1:00am January 25, 2015, LPD's computer network began to receive computer attacks, in particular, attempts to gain remote access to the internal contents of LPD's network. On January 26, 2015, the FBI spoke with LPD's Information Technology (IT) Administrator, Damon Weaver, and Mr. Weaver advised that around or about 1:00am the morning of January 25, 2015, LPD's network began receiving numerous attempts to access their networks via varied attacks methods, to include; Standard Query Language (SQL) injection attempts, Remote Desktop Protocol (RDP) attacks, Secure Shell (SSH) attacks, as well as others. Mr. Weaver advised that he was also aware that Longview City's network had been experiencing some computer attacks during the same time frame. Longview City's networks are housed and hosted at Rackspace in Dallas, in the Northern District of Texas.

3. On January 26, 2015, the FBI spoke with Longview City's IT Security Administrator, Josh Gamble. Mr. Gamble advised that Longview City's network had been receiving computer attacks in attempt to access their internal network, similar to the attacks against LPD's network. He also advised that Longview City's website, www.longviewtexas.gov, had been brought down several times by Distributed Denial of Service (DDoS) attacks. The website was initially brought down at, or around, 1:08am the morning of January 25, 2015.

4. On May 21, 2015, the FBI Denver Field Office served a search warrant on Twitter.com pursuant to a DDoS attack against the City and County of Denver in late January 2015. One of the Twitter.com accounts covered under the search warrant was @Solo_Sec, with Twitter User Identification (UID) number 2851728039. Review of the contents of the @Solo_Sec account revealed direct messaging between @Solo_Sec and Twitter.com account @Justice Seeker01, with UID 2796684332, regarding the shooting of Kristiana Coignard by LPD on, or about, February 1, 2015. @Solo_Sec and @JusticeSeeker01 had the following direct messaging conversation:

Identification Number (To)	Identification Number (From)	Date and Time	Text/Description
UID 2851728039 @Solo_Sec	UID 2796684332 @JusticeSeeker01	Feb 1, 2015 23:37	Target http://t.co/RpeLHplHOP for the shooting death of 17 y/o Kristiana Coignard by Longview Police Department. We need all of us on it ASAP
UID 2851728039 @Solo_Sec	UID 2796684332 @JusticeSeeker01	Feb 1, 2015 23:37	If you could get as many people together on this to help as possible it will be greatly appreciated.
UID 2796684332 @JusticeSeeker01	UID 2851728039 @Solo_Sec	Feb 1, 2015 23:47	Will do brother
UID 2851728039 @Solo_Sec	UID 2796684332 @JusticeSeeker01	Feb 1, 2015 23:49	thank you. new target is the news station that is spreading false information. http://t.co/rglTotKKQE pretty strong need lots of fire power

5. During the direct messaging conversation between @Solo_Sec and @JusticeSeeker01 on February 1, 2015, the account @Solo_Sec posted two public tweets to their account. Below are the two tweets by @Solo_Sec:

Date and Time	Text/Description
Feb 1, 2015 23:48	Target http://t.co/AT0cyWTPC6 Everything going to be bigger in Texas!
Feb 1, 2015 23:52	Target: http://t.co/mR7Z3Eiv71 #KLTV Were gonna have a #TangoDown shortly.

6. On January 12, 2016, Affiant visited the URL “[http://t.co/ AT0cyWTPC6](http://t.co/AT0cyWTPC6),” and it resolved to the website “www.longviewtexas.gov.”

7. On October 19, 2015, Affiant visited the Twitter.com site for the Twitter account @JusticeSeeker01 and observed several tweets posted on, or around, February 1, 2015. Below are the tweets by @JusticeSeeker01:

Date and Time	Text/Description
Feb 1, 2015	Target longviewtexas.gov for the shooting death of 17 y/o Kristiana Coignard by Longview Police Department. We need all of us on it ASAP
Feb 1, 2015	Target kltv.com why? For lying to the public about 17 y/o Kristiana Coignard’s murder by Longview Police.
Feb 1, 2015	Watch Justice for Kristiana on @Livestream:new.livestream.com/accounts/1460/...
Feb 1, 2015	Can you believe this...Longview kill a 17 y/o child and someone makes a sign telling them they Rock. (post of picture)

8. Affiant observed from review of the tweet above by @JusticeSeeker01 that requested people “Target Longviewtexas.gov for the shooting death of 17 y/o

Kristiana Coignard...,” that it was identical to the direct message from @JusticeSeeker to @Solo_Sec on February 1, 2015, at 23:57, requesting @Solo_Sec to “Target <http://t.co/RpeLHplHOP> for the shooting death of 17 y/o Kristiana Coignard....” The only difference between the tweet and the direct message was that the Uniform Resource Locator (URL) listed in the tweet was “Longviewtexas.com,” and the URL in the direct message was “<http://t.co/RpeLHplHOP>,” which is the format of how Twitter.com automatically converts some URLs. On January 12, 2016, Affiant visited the URL “<http://t.co/RpeLHplHOP>,” and it resolved to the website www.longviewtexas.gov.

9. On or about October 20, 2015 and again on January 21, 2016, Affiant requested that Twitter, Inc. preserve the information associated with the Twitter account @JusticeSeeker01, <https://twitter.com/justiceseeker01> pursuant to 18 U.S.C. § 2703(f).

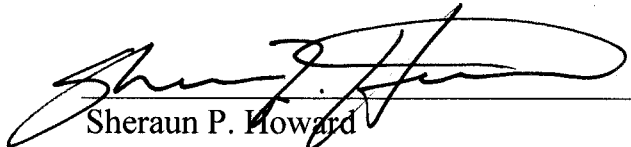
10. Based on the above events, there is probable cause to believe that in the Twitter account for @JusticeSeeker01, with the account address <https://twitter.com/justiceseeker01>, there is evidence that the owner of the @JusticeSeeker01 account has violated 18 U.S.C. §§ 1030(a)(5)(A).

CONCLUSION


11. Based on the foregoing, there is probable cause to believe that evidence of violations of 18 U.S.C. §§ 1030(a)(5)(A) exists on Twitter’s servers related to the account @JusticeSeeker01, with URL <https://twitter.com/justiceseeker01>, and I

request that the Court issue the proposed search warrant for the Twitter account **@JusticeSeeker01**, with URL **<https://twitter.com/justiceseeker01>**, as described on **Attachment A** and all Twitter records related to the account as described in **Attachment B**. Because the warrant will be served on Twitter, Inc. who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

Respectfully submitted,


Sheraun P. Howard
Special Agent
Federal Bureau of Investigation

Subscribed and sworn to before me on January 22, 2016.


PAUL D. STICKNEY
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A
Property to Be Searched

This warrant applies to information associated with the account
@JusticeSeeker01, with URL **<https://twitter.com/justiceseeker01>**, which is stored at
premises controlled by Twitter, Inc., a company that accepts service of legal process at
1355 Market Street, Suite 900, San Francisco, California 94103.

ATTACHMENT B
Particular Things to be Seized

I. Information to be disclosed by Twitter, Inc. (the "Provider")

To the extent that the information described in Attachment A related to the account @JusticeSeeker01, with URL <https://twitter.com/justiceseeker01> and is within the possession, custody, or control of the Provider, including any messages, records, files, logs, or information that has been deleted but is still available to the Provider, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f) (Reference # 00DA0000000K0A8.500G000000oznle), the Provider is required to disclose the following information to the government:

- a. All identity and contact information, including full name, e-mail address, physical address (including city, state, and zip code), date of birth, gender, hometown, occupation, and other personal identifiers;
- b. All past and current usernames, account passwords, and names associated with the account;
- c. The dates and times at which the account and profile were created, and the Internet Protocol ("IP") address at the time of sign-up;
- d. All IP logs and other documents showing the IP address, date, and time of each login to the account;
- e. All data and information associated with the profile page, including photographs, "bios," and profile backgrounds and themes;
- f. All "Tweets" and Direct Messages sent, received, "favorite," or retweeted by the account, and all photographs or images included on those Tweets and Direct Messages;
- g. All information from the "Connect" tab for the account, including all lists of Twitter users who have favorite or retweeted Tweets posted by the account, as well as a list of all Tweets that include the username associated with the account (i.e. "mentions" or "replies");
- h. All photographs and images in the user gallery for the account;

- i. All location data associated with the account, including all information collected by the "Tweet With Location" service;
- j. All information about the account's use of Twitter's link service, including all longer website links that were shortened by the service, all resulting shortened links, and all information about the number of times that a link posted by the account was clicked;
- k. All data and information that has been deleted by the user;
- l. A list of all the people the user follows on Twitter and all people who are following the user (i.e., the user's "following" list and "followers" list);
- m. A list of all users the account has "unfollowed" or blocked;
- n. All "lists" created by the account;
- o. All information on the "Who to Follow" list for the account;
- p. All privacy and account settings;
- q. All records of Twitter searches performed by the account, including all past searches saved by the account; and
- r. All information about connections between the account and third-party websites and applications.

II. All records pertaining to communications between Twitter and any person regarding the user or the users of the Twitter account, including contacts with support services, and all records of action taken, including suspensions of the account.

III. Information to be seized by the government

All information described above in Section I that constitutes evidence of violations of 18 U.S.C. §§ 1030(a)(5)(A) and 1030(b), including, for each account or identifier listed on Attachment A from account inception to present, information pertaining to the following matters:

- a. Communications between the account and any co-conspirators regarding computer intrusion activities, denial of service attacks, doxing or identity theft;

- b. Evidence indicating how and when the account was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crimes under investigation and to the account owner;
- c. Communications between the account and any co-conspirators providing information needed or used to further the conspiracy, or to aid and abet the criminal acts of others, in violation of the above statutes ;
- d. Evidence indicating the email account owner's state of mind as it relates to the crime under investigation, including information indicating motivation for intrusions (such as profit, damage, revenge or retaliation, intelligence gathering, etc.)
- e. The identity of the person(s) who created or used the account, including records that help reveal the whereabouts of such person(s).
- f. The identity of the person(s) who communicated with the account about matters relating to computer intrusions, denial of service attacks, doxing or identity theft, including records that help reveal their whereabouts.